



G Data Whitepaper

Behaviour Blocking

Marco Lauerwald
Marketing



Inhalt

1	Behaviour Blocking – Mission: Unbekannte Bedrohungen bekämpfen.....	2
1.1	Unbekannte Schädlinge: Die Malware-Industrie boomt.....	2
1.2	Sicherheitsstufen eines Computers mit AntiViren-Lösung.....	3
1.2.1	Die Sicherheitsstufen (Security Layer) beim Surfen	3
1.2.2	Die Sicherheitsstufen (Security-Layer) beim E-Mailen	4
1.3	Funktionsweise des Behaviour Blockers	4
1.4	Prüfungsprozess auf verdächtiges Verhalten	4
1.5	Beispiel: Der G Data Behaviour Blocker	5

1 Behaviour Blocking – Mission: Unbekannte Bedrohungen bekämpfen

Achtung, unbekannte Bedrohung! Wenn der PC diese Meldung anzeigt, können Computer-Anwender sicher sein, dass die eingesetzte Sicherheitslösung das Schlimmste verhindert hat: Verlust von privaten Daten und Passwörtern oder das Verschicken von Spam-Mails über das eigene E-Mailkonto. Viele Anwender fühlen sich durch ihre Antiviren-Software vor Malware geschützt. Ein umfassender Schutz besteht aber nur dann, wenn auch sogenannte Zero-Day-Attacken – also unbekannte Malware-Angriffe – verhindert werden können. Der Behaviour Blocker greift an genau dieser Stelle: Er erkennt unbekannte Bedrohungen für die es noch keine Virensignaturen gibt anhand ihres verdächtigen Verhaltens und schaltet sie aus.

In diesem Whitepaper wird beschrieben, wie diese Technologie funktioniert und welche Vorteile der Behaviour Blocker für den Anwender hat.

1.1 Unbekannte Schädlinge: Die Malware-Industrie boomt

Im zweiten Halbjahr 2010 stieg die Anzahl an neuen Computerschädlingen¹ auf 1.076.236. Das sind durchschnittlich 5.840 pro Tag. Insgesamt sind 2010 mehr als zwei Millionen neue Varianten von Schadprogrammen aufgetaucht (vgl. Diagramm 1) – 32 Prozent mehr als 2009 und fast 52 mal mehr als 2006. Bereits im ersten Halbjahr 2010 gab es mehr neue Schädlinge als im gesamten Jahr 2008.

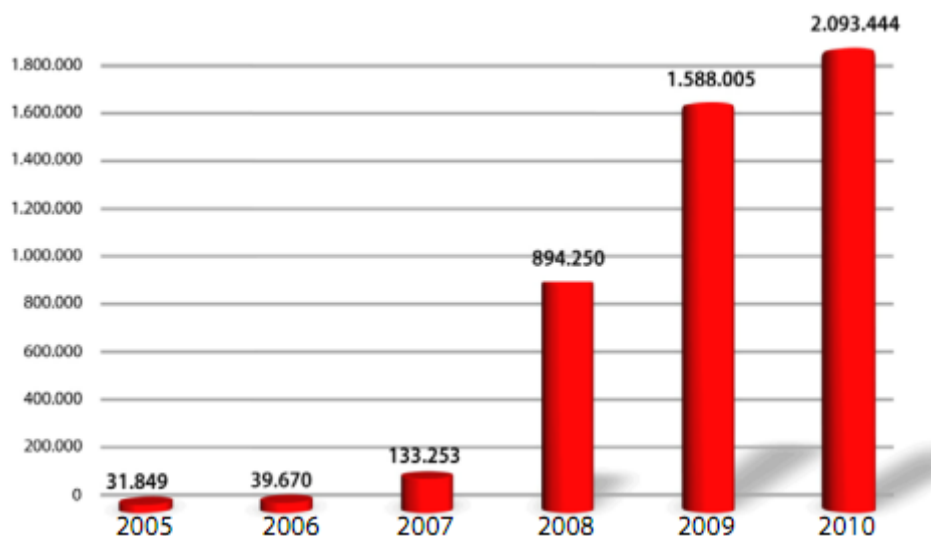


Diagramm 1: Anzahl neuer Malware pro Jahr seit 2005

Die Malware-Industrie boomt und auch bislang unbekannte Bedrohungen müssen bekämpft werden. Hier fungiert der Behaviour Blocker als letzter Schutzmechanismus im Sicherheitskonzept beim Surfen oder E-Mailen.

¹ Vgl. G Data MalwareReport 02/2010

1.2 Sicherheitsstufen eines Computers mit AntiViren-Lösung

Mit einer installierten Antiviren-Lösung ist der Computer über verschiedene Sicherheitsstufen (Security Layer) optimal geschützt. Nachfolgend werden diese Mechanismen beim Surfen und E-Mails näher beschrieben und erläutert:

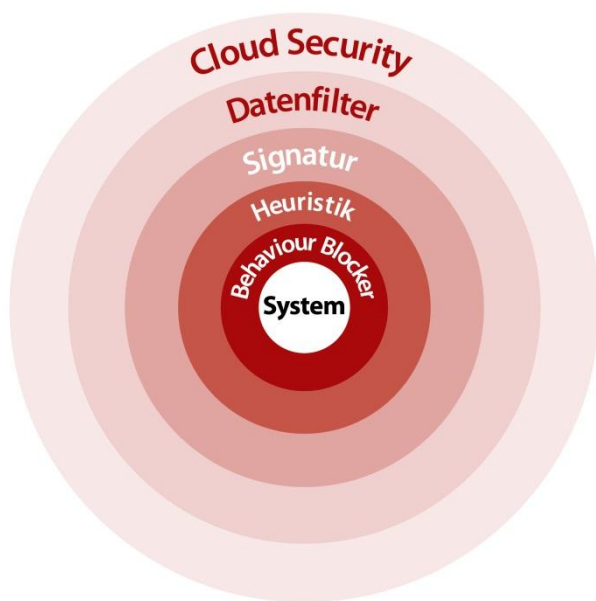


Abbildung 1: Übersicht der Sicherheitsstufen eines Computers mit einer Antiviren-Software

1.2.1 Die Sicherheitsstufen (Security Layer) beim Surfen

Grade beim Surfen im Internet infizieren sich viele Nutzer mit schädlicher Software. Eine Sicherheits-Software kann mithilfe der verschiedenen Sicherheitsstufen eine Infektion vermeiden und mithilfe des Behaviour Blockers sogar vor unbekanntem Schädlingen schützen:

Layer	Methode	Effekt
Web Cloud	vergleicht URLs mit Blacklist bekannter schädlicher URLs	blockt bekannte infizierte / betrügerische Webseiten
http-Filter	scannt http-Traffic beim Download	blockt bekannte Malware
Viren-Wächter (Signatur)	scannt Dateien beim Zugriff gegen bekannte Virensignaturen	blockt bekannte Malware
Viren-Wächter (Heuristik)	scannt Dateien beim Zugriff gegen generische Signaturen	blockt unbekannte Malware-Varianten
Behaviour Blocker	prüft Verhaltensmuster auf virentypische Eigenschaften	blockt unbekannte Malware

1.2.2 Die Sicherheitsstufen (Security-Layer) beim E-Mailen

Beim Versenden und Empfangen von E-Mails können unbekannte Bedrohungen auftreten.

Layer	Methode	Effekt
Mail Cloud	gleicht Fingerprints von Mails mit dem weltweiten Mail-Traffic ab	blockt Outbreaks infizierter Mail bzw. Spam-Mails
Mail Filter	scannt Mails beim Empfang	blockt bekannte Malware
Viren-Wächter(Signatur)	scannt Dateien beim Zugriff gegen bekannte Virensignaturen	blockt bekannte Malware
Viren-Wächter (Heuristik)	scannt Dateien beim Zugriff gegen generische Signaturen	blockt unbekannte Malware-Varianten
Behaviour Blocker	prüft Verhaltensmuster auf virentypische Eigenschaften	blockt unbekannte Malware

1.3 Funktionsweise des Behaviour Blockers

Der Behaviour Blocker ist ein Schutzmechanismus, der das Verhalten von ausgeführten Programmen beobachtet und gegebenenfalls blockiert. Programme, Downloads und andere Dateien versuchen beim Start verschiedenste Aktionen auf dem Computer durchzuführen. Bei der Einordnung eines Programms in die Kategorie „Bedrohung“, spielen vor allem das Zusammenspiel und die Art der ausgeführten Aktionen eine Rolle.

Folgende Verhaltensweisen² können unter anderem dazu führen, dass eine Software als potentielle Bedrohung für die Computer-Sicherheit angesehen wird:

- Autostart-Einträge aller Art, ob durch Ablegen von Dateien im richtigen Ordner oder manipulierte Registry-Werte
- .exe oder .dll-Dateien, die sich in das system32-Verzeichnis kopieren
- Einträge, die die Registry-Werte manipulieren, welche die Sicherheit des Systems betreffen
- Verhaltensweisen, die Einstellungen für den Internet Explorer ändern
- Veränderungen von hosts-Dateien
- Code Injection – Programmcode im Kontext eines anderen Programms ausführen (z. B. um Firewalls zu umgehen, indem der Code im Kontext des Internet Explorer läuft)
- Durch ExePacker gepacktes Programm (um Signaturfilter zu umgehen)
- Beschädigte (aber trotzdem ausführbare) Programmdateien

1.4 Prüfungsprozess auf verdächtiges Verhalten

Der G Data Behaviour Blocker ist auf einem regelbasierten Expertensystem aufgebaut. Dabei werden Verhaltensregeln manuell erstellt und angepasst, wodurch Erkennungs- und False-Positive-Raten optimiert werden. Wird ein Programm ausgeführt, werden die entstehenden Verhaltensweisen zu einer allgemeinen Aktion abstrahiert. Auf die Gesamtmenge der sogenannten Aktionen werden

² Exemplarische Beispiele

dann die Regeln angewandt, um weitere Eigenschaften und zuletzt einen einzelnen Wert für die Gefährlichkeit abzuleiten. In diesem Prozess werden bestimmte und immer wieder auffällige Kombinationen besonders beachtet.

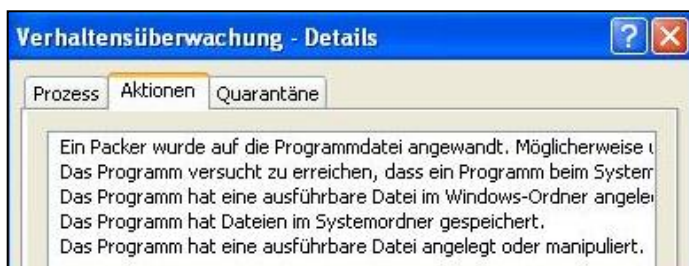
1.5 Beispiel: Der G Data Behaviour Blocker

Ist ein Programm mit einem Schädling versehen und zeigt deshalb mehrere der oben beschriebenen Verhaltensweisen, wird es vom G Data Behaviour Blocker als „Unbekannte Bedrohung“ eingestuft und geblockt:



Screenshot 1: Wird eine verdächtige Aktion ausgeführt, schaltet sich die G Data Verhaltensüberwachung ein.

Der Anwender muss jetzt entscheiden, wie er mit der Bedrohung umgehen möchte. An dieser Stelle ist es in der Regel ratsam, das schädliche Programm in die Quarantäne zu verschieben. Unter Umständen können allerdings manchmal auch schadfremde Programme als gefährlich eingestuft werden. Deshalb ist es zu empfehlen, einen Blick in die Details zu werfen und zu schauen, aus welchem Grund das Programm gestoppt wurde:



Screenshot 2: Detailansicht der Verhaltensüberwachung.

Es ist generell sinnvoll, Programme nicht einfach blind zu installieren. Jeder Anwender sollte den Sinn und Zweck, sowie die Herkunft genau hinterfragen.

Der Behaviour Blocker fungiert als Schutz vor unbekanntem Bedrohungen, kann alleine aber auf keinen Fall die anderen Komponenten einer Antiviren-Lösung ersetzen. Es ist besonders wichtig, Malware bereits als solche zu erkennen, bevor der Behaviour Blocker aktiv werden muss.